NPS-CS-09-006

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

A Preliminary Study of Barriers to Engagement in CyberCIEGE

by

Janne Hagen, Cynthia E. Irvine, and Michael F. Thompson

May 2009

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Daniel T. Oliver
President

Leonard A. Ferrari
Executive Vice President and
Provost

This report was partially supported by the Biometrics Task Force.

This report was prepared by:

_____
Janne Hagen
Visiting Research Associate

_____
Cynthia E. Irvine
Professor
Department of Computer Science

Reviewed by:

_____
Peter J. Denning
Chair
Department of Computer Science

Released by:

_____
Karl van Bibber
Vice President and
Dean of Research

REPORT DOCUMENTATION PAGE

Form approved

OMB No 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	24 May 2009	Research; 7/1/08 – 5/12/09

4. TITLE AND SUBTITLE

A Preliminary Study of Barriers to Engagement in CyberCIEGE

5. FUNDING

MIPR8JBIOM0075
MIPR8JBIOM0112

6. AUTHOR(S)

Janne Hagen, Cynthia E. Irvine, Michael F. Thompson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School
Center for Information Systems Security Studies and Research (NPS CISR)
1411 Cunningham Rd., Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

NPS-CS-09-006

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Biometrics Task Force
Army G3/7, Crystal Mall 4, 1901 South Bell St., Arlington, VA 22202

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

Not applicable

11. SUPPLEMENTARY NOTES

The views expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words.)

CyberCIEGE is a resource-management simulation in which the player assumes the role of a decision maker for an IT-dependent organization. Through the use of scenarios, it is intended to support education, training and awareness in cyber security. Naval Postgraduate School (NPS) plans to use the game to help to teach Identity Management concepts. To help prepare for that, we conducted a study of barriers to engagement in CyberCIEGE by observing eight students while playing the game, analyzing game logs and holding evaluation meetings with two classes. Our study revealed several barriers to becoming engaged in the game due to weaknesses in the game's user interface, the students' limited understanding of the security context and their limited video game playing skills. These problems can be mitigated by structuring game scenarios so that students must pass the beginners' level before advancing to subsequent levels. Optimally, a skilled student should be allowed to skip the simple introductions; however, it is not clear that student skill can be reliably assessed prior to playing the scenarios. Also, the CyberCIEGE Tire Ply Scenario should be improved to provide unambiguous objectives, timely and clear feedback and more relevant real life narratives.

14. SUBJECT TERMS

Cyber Security, Information Assurance, Education, Video Games

15. NUMBER OF PAGES

26

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NAVAL POSTGRADUATE SCHOOL
CENTER FOR INFORMATION SYSTEMS SECURITY STUDIES AND RESEARCH

Technical Report NPS-CS-09-006

A Preliminary Study of Barriers to Engagement in CyberCIEGE

Janne Hagen, Cynthia E. Irvine, Michael F. Thompson

May 24, 2009

NPS-CS-09-006

Acknowledgements

This work was sponsored, in part, by the Identity Management Education Program at the Naval Postgraduate School, which is grateful to the Biometrics Task Force for its generous support of Identity Management Education. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Identity Management Program or Naval Postgraduate School.

The authors would like to thank the students, who contributed with data to this study.

Author Affiliation

Center for Information Systems Security Studies and Research
Department of Computer Science
Naval Postgraduate School
Monterey, California 93943
U.S.A

Abstract

CyberCIEGE is a resource-management simulation in which the player assumes the role of a decision maker for an IT-dependent organization. Through the use of scenarios, it is intended to support education, training and awareness in cyber security. Naval Postgraduate School (NPS) plans to use the game to help to teach Identity Management concepts. To help prepare for that, we conducted a study of barriers to engagement in CyberCIEGE by observing eight students while playing the game, analyzing game logs and holding evaluation meetings with two classes. Our study revealed several barriers to becoming engaged in the game due to weaknesses in the game's user interface, the students' limited understanding of the security context and their limited video game playing skills. These problems can be mitigated by structuring game scenarios so that students must pass the beginners' level before advancing to subsequent levels. Optimally, a skilled student should be allowed to skip the simple introductions; however, it is not clear that student skill can be reliably assessed prior to playing the scenarios. Also, the CyberCIEGE Tire Ply Scenario should be improved to provide unambiguous objectives, timely and clear feedback and more relevant real life narratives.

Table of Contents

This page is intentionally blank.

1 Introduction

CyberCIEGE is a resource-management simulation in which the player assumes the role of a decision maker for an IT-dependent organization. The objective is to keep the organization's virtual users happy and productive while providing the necessary security measures to protect valuable information assets. With good choices, the organization prospers and the scenario advances; poor choices often result in disaster (Irvine, Thompson and Allen, 2005). The CyberCIEGE game has been made available at no cost to the US government agencies and more than 130 schools and universities. The game is being extended to support education in identity management concepts.

Even though current research shows promising results from the use of video games and simulation technology in teaching, and also gives some guidance regarding factors that sustain players' engagement (Michell and Savill Smith, 2004: Dondlinger, 2007), it is not obvious that all these results are relevant to the teaching of computer security in general and the learning objectives of CyberCIEGE in particular.

CyberCiege is designed to support training and awareness as well as information assurance education. With respect to training and awareness, Cone, Irvine, Thompson and Nguyen (2007) claim that the initial test results of the basic user training scenario in CyberCIEGE are positive and that CyberCIEGE is useful in supporting information security awareness programs.

Use of CyberCIEGE for education requires a deeper level of student engagement than is needed for awareness training. Fung, Khera, Depckere, Tantatsanawong and Boonbrahm (2008) conducted a pilot study among a small group of Thai students on the learning effects of CyberCIEGE. They found that students, who successfully completed the game, appeared to be able to demonstrate a deeper level of understanding compared with those who just attended class lectures. Moreover, their findings showed that some students did not complete the game, yet there were no detailed reasons provided regarding the cause of the withdrawals except boredom. Our study aims to explore further why students drop out by asking the following questions:

1) What barriers do the players of CyberCIEGE face when it is used for education?

2) How can the barriers and drawbacks be categorized: experience based, knowledge based, based on the game design, or other factors?

3) How can these barriers and drawbacks be mitigated in order to improve the utility of CyberCIEGE in computer security education? For example, could pre-training, changes to the design of the user interface, or other techniques improve student tenacity?

We have analyzed game logs, conducted observational studies of eight students, and collected information from two in-class meetings to answer these questions.

The next section gives a short introduction to CyberCIEGE and the Tire Ply Filter Scenario that was used in this study. Section three reviews current research regarding the motivation of players' engagement in educational games. Section four presents the methods and data and section five is an analysis of our findings. Section six discusses our results relative to other work on the use of video games in education and section seven ends this paper with our conclusions and recommendations for further work.

2 The CyberCIEGE Tire Ply Filter Scenario

CyberCIEGE scenarios are organized in a sequence where vulnerability risks and mitigations become increasingly complex from one scenario to the next. For example, the CyberCIEGE identity management scenarios were developed to help teach identity management concepts, including the use of biometrics to control and track physical access to a military base. The design of these scenarios was predicated on the assumption that the student will have played the CyberCIEGE Tire Ply Filters scenario first.

Because it is a stepping-stone toward more advanced scenarios, the Tire Ply Filters scenario was selected to undergo evaluation in this study. In addition, it includes much of the mechanics needed for the more advanced scenarios, such as those for Identity Management, yet it is somewhat simpler.

The Tire Ply Filters scenario explores issues arising from connecting networks to the Internet and the use of network filters to protect internal assets. It consists of four phases, which are described briefly below:

Phase 1 requires the player to provide a game character with access to the Internet. The player is expected to buy a router and then connect the virtual user's computer to the Internet. Phase 2 is about setting the router's filters to prevent direct attacks from the Internet. This phase has a simple solution, which is to deny all application service requests from the Internet. Phase 3 starts when the different game character, Mary, who begins working on a very valuable asset. The player is expected to disconnect her computer from the Internet.

The last, and fourth, phase includes a government regulator at a remote location who needs access to one of the enterprise assets using a specific application. The student is expected to open the port for incoming SSH traffic through the network filter.

Player *help* in CyberCIEGE includes: tutorials, such as short animations to explain firewalls and filters; and an encyclopedia that explains all aspects of game operation. Scenarios can present instructive pop-up windows and tickers to the player. Finally, scenarios can be designed so that it is difficult for users to make mistakes, thus forcing them through a correct sequence of actions.

3 Player engagement and motivation

This section gives a brief review of research intended to determine how computer game players are engaged and motivated.

Medina (2005) argues that motivation theory provide a framework to study how users engage in playing both commercial games and educational games. Referring to Malone, she argues that domain competence influences the enjoyment of playing the game and that research has shown that fantasy, a game feature, stimulates players by both catching and holding their attention while playing over time (see Lepper and Corova, 2000). A distinction is made between extrinsic fantasies that depend only weakly on the skill used in a game, and intrinsic fantasies that are intimately related to the use of the skill. Curiosity is separated into sensory and cognitive components, and it is suggested that cognitive curiosity can be aroused by making learners believe their knowledge structures are incomplete (Malone and Lepper, 1987). Thus motivation seems to be a key factor for active involvement, in time and mind in the learning process: A

motivated learner can't be stopped (Denis and Jouvelot, 2005). Motivated learners are easy to describe: they are enthusiastic, focused and engaged (Garris, Ahlers and Driskell, 2002). Video games provide effective motivation because they are fun, a potent source of intrinsic motivation (Denis and Jouvelot, 2005).

Wishart (1990) conducted an experiment using primary school children. The results recorded by the computer during the experiment, showed that being in control of the program was most important in creating involvement with it. Introducing challenge and complexity separately did not increase involvement significantly. However, the children became more deeply involved when the program contained both complexity and challenge (Wishart, 1990). Tuzun (2003) used ethnographic methods in his studies with children and obtained thirteen elements that motivated them to play the game: identity presentation, social interaction, playing, learning, ownership and control, fantasy, immersive context, curiosity, creativity, achievements, rewards, uniqueness and context of support (Tuzan, 2003).

The literature on how players become engaged is intertwined with motivation theories and learning. *Ludology* focuses on the study of computer games as play and game activities, while *narratology* revolves around the study of computer games as narratives. While narratologists want to examine how one can tell a good story in games where the result is not a winner or a looser, ludologists choose to study a game's rules and mechanisms as analogous to those of a book: the interaction between text and reader, and ways to make the page flipping experience or text interaction more interesting. Ang and Rao (2008) conducted a survey on 100 students and found that both story telling and interaction contributed to the enjoyment of educational games.

A number of distinct design elements such as narrative context, rules, goals, rewards, multisensory cues, and interactivity, seem necessary to stimulate desired learning outcomes (Dondlinger, 2007). There is, however, little consensus on the process by which games engage learners (Garris, Ahlers and Driskell, 2002).

Garris et al. (2002) argue that material may be learned more readily when presented in imagined contexts that are of interest rather than in a generic decontextualized form. One of the most robust findings in the literature on motivation is that clear, specific, and difficult goals lead to enhanced performance. Clear, specific goals allow the player to perceive goal-feedback discrepancies, which are seen as crucial in triggering greater attention and motivation. Players are challenged by activities that are neither too easy nor too difficult to perform. Also, students' control leads to greater motivation and learning (Garris, Ahlers and Driskell, 2002).

4 Methods and data

We have applied a research design mainly based on observational studies and qualitative interviews. The next sections give a description of the applied methods, data and limitations.

4.1 The research design

As one of its laboratory exercises, an introductory computer security course at the Naval Postgraduate School uses CyberCIEGE. We conducted an in-depth observation of the game interactions of eight students and subsequently met with two class sections, in which all of the students had played CyberCIEGE. In addition we analyzed log files from 34 students. Our in-depth study of eight student subjects is discussed first.

Each student was observed individually in a quiet setting with no distractions. Initially, the students answered a set of questions about their experience in gaming and their knowledge of computer security. Then students who had not already completed a tutorial on the use of firewalls and information filtering were asked to watch the movies. This tutorial is an introductory movie entitled "Security Basics: Firewalls," and is available as part of the collection of resources provided to players in a standard CyberCIEGE distribution. The reason students were asked to watch the movies was to ensure that all students began playing the Tire Ply Filters with a common minimum amount of background knowledge. These were followed by CyberCIEGE sessions in which the students played the Tire Ply Filters scenario.

During the CyberCIEGE sessions, the students were encouraged to express their thoughts and actions related to their experience with the game. The aim of this activity was not to investigate how well they played the game, but to investigate how playing CyberCIEGE challenged and engaged them, how they reacted to upcoming problems posed in the scenario, and how they used the game's *help* functionality. The investigator observed the students' interactions with the game, and took notes. Before each session closed the investigator asked the student to describe was aspects of the game that were most difficult and how the student solved the problems associated with that difficulty. Students were asked open-ended as well as pointed questions. This allowed the participants to provide both broad assessments of their game playing experiences, as well as answers to specific questions.

Each observation and interview was documented. In addition to the written summaries of the interviews and observation, the logs created from CyberCIEGE were used in the analysis.

When five of the students (approximately half of the group) had been through CyberCIEGE game playing, observations and interviews, the written summaries were analyzed and the following hypotheses about challenges to engagement in CyberCIEGE were developed:

1) Playing the introductory scenario helps students with user interface challenges.

2) Experienced players are more engaged in the game.

3) Players with a good understanding of the security context are more engaged in the game.

Then, the next three students went though the same sessions, but now the observations also focused on the developed hypotheses. These students were also helped actively if they were unable to make progress while playing the game. Each session took about one hour per student.

A 30-minute meeting was arranged with two classes at NPS that had played the CyberCIEGE game. The objective of the discussion was partly to validate our findings, but also to reveal any undetected challenges and to brainstorm possible improvements to the game. The meeting included small group discussions and discussions in plenum.

4.2 Limitations

The major weakness in this study is the low number of observations. It is, however, our opinion that the eight participants provided some variety regarding the kinds of students who might play CyberCIEGE. When combined with the log files and the in-class discussions, these elements provided us with insight into how the players interacted with the game and how they were engaged or frustrated.

The findings are presented in the next section.

5 Findings

5.1 Playing patterns

In addition to observing the eight students play the game, we analyzed logs from 34 previous students playing the Tire Ply Filters scenario in the CyberCIEGE game. The result shows that 25% of the students lost the game or quit prior to completing all phases of the Tire Ply Filters scenario. On average, winners spent 12 minutes on playing the scenario compared with those who lost or decided to quit, who spent 8 minutes on playing. The logs showed that the average winner restarted the Tire Play Filters scenario four times, whereas the average player who lost or quit restarted only three times. The winners appear to make more tries for two reasons: 1) They do not give up and 2) they experiment and explore the game even after winning.

5.2 Type of game players

We identified two types of video game players: 1) The experienced game player who has played a variety of games and still enjoys playing at least now and then and 2) the novice player with limited previous experience in playing computer games. We also identified two groups of students with different security context knowledge: 1) Those with excellent knowledge who have both practical skills and good theoretical insight, and 2) intermediate students, whose security knowledge and practical skill ranged from limited to intermediate. The latter constituted the majority of the students in our study.

5.3 Different students faced different challenges

The categorization of players' experience with video games and computer security found in Section 5.1 enables us to produce a matrix to study the challenges the players faced. Observations regarding different combinations of player characteristics are located in each cell of the matrix, which is illustrated in Table 1. This revealed a picture of the challenges different kinds of students met while playing the CyberCIEGE game.

Table 1 Challenges of playing CyberCIEGE

	Experience	
Security Context Understanding	**Novice Player**	**Experienced Player**
Intermediate Understanding	Overwhelmed by the user interface, did not understand the game's objectives	Expected a simpler user interface, or one more closely resembling other games did not understand the objectives
Excellent Understanding	Overwhelmed by the interface, and thought further than expected by the game	Expected a simpler interface, or one more closely resembling other games, and thought further than expected by the game

Grouping our first five observations into this framework also revealed that the only player of the five who successfully played the game, was both an experienced game player and had excellent computer security skills. The other four students fit into the other categories and none managed to finish the game within the time available. However, the last three of the eight students were successful. They were given help, such as first playing the Phase 1 of the Introductory Scenario that walks the player through some basic mechanics interface of the game, and through the provision of oral hints after the student had been stuck at least 1 minute with a problem.

5.4 Classes of challenges

Both the experienced and novice players had problems with the user interface: how to do things, where to find information and game navigation. Few of them took their time to read the recommended introductory information provided or study the encyclopedia, which comes with the game. Thus, the learning curve was considered to be steep for both groups, but the experienced game players explored and worked faster than the novice players. They also expected the game to behave the way other games behaved, thus some were disappointed, particularly when their game playing experience was limited to fundamentally different game genres. Sometimes feedback was considered to be too instantaneous, for example, they were charged dollars for selecting the different security options and felt that this should be permitted without being charged. In other cases, the feedback was too slow, for example, after making choices, the students had to run the simulation for a while before the game would provide the student with feedback (e.g., notification of a successful attack against an asset.)

The players' ability to interpret and understand what they were expected to do to achieve the game's objectives was influenced by the players' computer security knowledge. For example, those who had trouble conceptualizing the function of a network filter were distracted by tangential questions about network protocols.

After observing the game play, we asked the players for their evaluation of the fun, humor, variety and complexly in the game. Five of the observed players found the game fun to play, and noted that the way the characters spoke and behaved was humorous. Three players did not see much fun in it. As expected, the attitude towards the complexity of the game depended on the skill and contextual security knowledge of the player. Table 2 summarizes the fun factors and the motivation to go on playing. The table shows that students with a good contextual understanding of computer security wanted to continue playing.

Table 2 The fun factor and motivation to continue to play the game

	Experience	
Security Context Understanding	**Novice Player**	**Experienced Player**
Intermediate Understanding	Not fun, unsure about going on playing	Not fun, stop playing
Excellent Understanding	Fun, continue playing	Easy and fun, continue playing

5.5 Student game improvements suggestions

The eight observed students gave advice for improvements to the game, and these suggestions were confirmed by the two class meetings the students. Table 3 summarizes these suggestions.

Table 3 Suggested improvements by the different player categories

	Experience	
Security Context Understanding	**Novice Player**	**Experienced Player**
Intermediate Understanding	More advice and adequate feedback on failures	Multilevel scenarios, more dedicated advice and timely feedback
Excellent Understanding	Show the objectives first	Multi-tasks phases and multi level scenarios, competitive driven game

Leveling the scenarios as “beginner”, “intermediate” and “advanced”, so that they are appropriate for different student groups was one suggested solution. Some suggested testing the students as part of the game, and then link them to their correct starting level. The advanced players with excellent knowledge were not challenged at all. This suggests that the game should be open for more awards if played better than expected. Some of the experienced players also wanted a higher degree of competition in the game such as displaying the average and high scores, (in terms of remaining cash at the end of the scenario) recorded from previous student play.

Some students suggested that the scenario narrative, could be made more relevant regarding how things work in the real life; e.g., do not disconnect a computer and use it for secret data processing, rather buy a new computer and never connect it to the Internet, or use a secure trusted network.

The novice players requested better advice and timely feedback, also on wrong choices. They suggested that the objectives should be to the point and unambiguous, and displayed. Additional realism was also suggested.

6 Discussion

Two major challenges confront the designers of educational video games. The first is that of player motivation: how can the game be organized so that the student will play long enough to learn the basic concepts of video game play? The second is one of designing scenarios and games so that a broader student population is reached.

6.1 The challenge of motivation and engagement

Malone and Lepper (1987) and Medina (2005) have discussed what contributes to making game players engaged and motivated. Engaged and motivated players are easy to see, and they do not stop playing (Dennis and Jouvelot, 2005; Garris et al, 2002). Fun is regarded as a potent source of intrinsic motivation that influences engagement. Our data shows that different categories of players have different views regarding the fun in CyberCIEGE, and this view correlates with their desire to continue playing the game. It seems like having a good understanding of computer security is important (Table 2) for also detecting any humor in the game and becoming engaged and motivated. This is in line with the findings of Garris et al (2005), who claim that clear specific goals and students’ exercise of ability to regulate or direct or command something, leads to greater motivation. One lesson learned could be that CyberCIEGE should not be introduced until the students have some basic introduction to information security management and resource administration. Another solution is to provide a variety of scenarios depending on the student’s initial skills and knowledge, as suggested by the students themselves. Assessment of each student’s initial knowledge and skills could allow placement of the start of play at the appropriate level of the game in terms of skills and knowledge. In addition, the goals could be simplified and made unambiguous.

Ang and Rao (2008) found that both narratology and ludology contributed to the enjoyment factor of educational games. The students in our study gave feedback on making the scenario (i.e. the narrative) more relevant for the audience; this included making the scenarios more realistic. Looking to the theory of ludology (see Ang and Rao, 2008), CyberCIEGE allows

players to save scenarios at the end of each completed phase. This lets the players move back into previous phases of the scenario. Furthermore, the choice the player takes does allow different paths regarding how the rest of the scenario will develop. There is a one-way path to the end, so to say, and after trying this path, there may not be much excitement in trying once again – players know what to do and the outcome is already known.

Several students suggested that the game would benefit from having the clear and unambiguous objectives presented first and then making the objectives available for viewing without leaving the main office screen.

The user interface of CyberCIEGE contributes to both its challenges and complexity. Several screens give a lot of information, and many students experienced this as "information overload". This should be balanced with the provision of adequate and timely feedback when mistakes are made.

6.2 The challenge of designing good scenarios and games

Our study shows that the way CyberCIEGE is designed at the moment, do not suit all students. Engagement and motivation varies among the different students depending on their knowledge of the security context and their skills in video game playing. Denis and Jouvelot (2005) claim that motivation is effective in video games because it deals with fun. But our study also shows that those students without good understanding of security context do not have fun playing the game, and are thus not engaged.

The game is designed to force players to complete simple scenarios leading up to more complex scenarios, providing pop up help as they encounter new operations. We had been disabling the setting that forces students to complete prerequisite scenarios prior to playing the Filters scenario. The study suggests that this feature should not be disabled. The study also suggested that the Filters scenario would benefit from additional pop up help to introduce players the concept of a router and to the mechanics of setting the filter.

We would suggest that CyberCIEGE should be further developed so that it first trains the players in the user interface, by playing some simple scenarios teaching them how to choose and what consequences different choices might have. A sequence of steps could be applied. First players could be introduced to the user interface. Then they could be trained on security concepts first by introducing simple challenges, and then progressing to a more advanced level. A skilled student should be able to skip the simple introductions and start with more advanced scenarios.

The user interface problems with the Tire Ply Scenario and the game pointed out by the students in this study, should as far as possible, be mitigated. But, because of the low number of observations, this does not guarantee that new students would not come up with new problems. A continuous evaluation process of CyberCIEGE could improve the game and the scenarios over time.

7 Conclusion

It has been suggested that CyberCIEGE is usable in supporting awareness programs. (Cone et al., 2005) However, some students do not complete the game. Our study explored this drop out problem.

We found that the students face several barriers related to the user interface of the game, their knowledge of computer security and their game playing skills. The barriers are categorized and vary according to the students' computer security knowledge and game playing skills.

The barriers can be mitigated by first introducing the players to the CyberCIEGE user interface, by playing some simple scenarios that teach students how to make choices and the consequences of various choices. Then more advanced scenarios should be introduced. Skilled players with good computer security knowledge should be allowed to skip the simple first phase. Also, the CyberCIEGE should be improved as suggested by the students regarding unambiguous objectives, timely and clear feedback, and a more relevant real life narratives. Finally, it is a good idea to reduce the time between the student's first introduction to CyberCIEGE and the lab exercise when the students play the Tire Ply Filters Scenario.

References

Ang, C. S. and Rao, G. S. V. "Computer Game Theories for Designing Motivating Educational Software: A Survey Study", International JI. On E-Learning (2008) 7 (2), 181-199.

Cone, B. D., Irvine, C. E., Thompson, M. F., Nguyen, T. D., "A Video Game for Cyber Security Training and Awareness", Computers & Security 26 (2007) pp. 63-72

Denis, G and Jouvelot, P. "Motivation-Driven Educational Game Design: Applying Best Practices to Music Education, ACE 2005, Valencia, Spain

Denis, G and Jouvelot, P. "Motivation-Driven Educational Game Design: Applying Best Practices to Music Education, ACE 2005, Valencia, Spain

Dondlinger, M, "Educational Video Game Design: A review of the Literature", Journal of Applied Educational Technology, 4(1): 21-31.

Fung, C.C, Khera, V, Depickere, A., Tantasanawong, P and Boonbrahm, P, "Raising information Security Awareness in Digital Ecosystem with Games – a Pilot Study in Thailand", 2008 Second IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2008), pp 375-380.

CyberCIEGE tutorials, http://cisr.nps.edu/cyberciege/movies.html.

Garris, R., Ahlers, R. and Driskell, J.E, "Games, motivation and learning: A research and practice model", Simulation & Gaming, 33 (4), December 2002: 441-447.

Irvine, C.E., Thompson, M.F., Allen, K.,"CyberCIEGE: Gaming for Information Assurance", Naval Postgraduate Sch., Monterey, CA, USA; Security & Privacy Magazine, IEEE, May-June 2005, Volume: 3, Issue: 3, page(s): 61- 64, ISSN: 1540-7993

Lepper, M. R. and Cordova D.I., " Intrinsic motivation and the process of learning: beneficial effects in the contextualization, personalization, and choice", in Journal of Education Psychology, 88 (4), 1996: 715-730.

Malone, T.W, "Toward a theory of intrinsically motivating instruction", Cognitive Science, 5 (4), 1981: 333-369.

Malone, T.W and Lepper, M.R, “Making learning fun: A taxonomy of intrinsic motivations for learning.” In R.E. Snow and M.J. Farr (eds), Aptitude, learning and instruction, Vol 3, Conative and Affective Process Analysis, 1987: 223-253.

Medina, E., “Digital Games: A motivational perspective. Presented at Digital Games Research Conference: DIGRA ‘05”, Vancouver, British Columbia, Canada.

Mitchell, A. and Savill-Smith, C, “ The use of computer and video games for learning. A literature review”, Learning and Skills Development Agency, UK, ISBN-1-85338-904-8, 2004, pp 44-45.

Tuzun, H, “Motivating learners in educational computer games”, Paper presented at the National Convention of the Association for Educational Communications on Technology, 2003: 465-475.

Tuzun, H. Lee, S.M., Graham, C. and Sluder, K.J, “Usability testing of the Indiana University Education Faculty Web Forms”, In: Annual Proceeding of Selected Research and Development, Vol 1-2 .

Wishart, J, “Cognitive factors related to user involvement with computers and their effects upon learning from an educational computer game”, Computers & Education, 15 (1-3), 1990: 145-150.

This page is intentionally blank.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218
2. Dudley Knox Library, Code 013 1
   Naval Postgraduate School
   Monterey, CA 93943
3. Research Office 1
   Naval Postgraduate School
   Monterey, CA 93943
4. Janne Hagen 2
   Department of Computer Science
   Naval Postgraduate School
   Monterey, CA 93943
5. Cynthia Irvine 2
   Department of Computer Science
   Naval Postgraduate School
   Monterey, CA 93943
6. Michael F. Thompson 2
   Department of Computer Science
   Naval Postgraduate School
   Monterey, CA 93943

This page is intentionally blank